

How resilient is Switzerland?

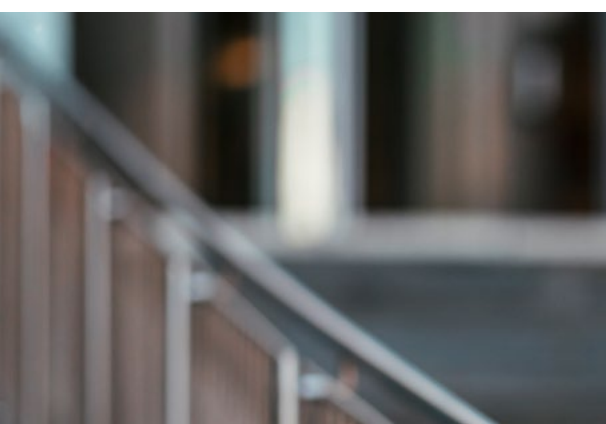
Interview with Dr. Myriam Dunn Cavelty, Deputy Director of the Think Tank at the Center for Security Studies (CSS), ETH Zurich

Cyberattacks, power shortages, geopolitical dependencies and AI highlight the close links between technical, societal and economic risks today. In a conversation with KPMG's Prof. Dr. Reto Eberle and Dr. Matthias Bossardt, Dr. Myriam Dunn Cavelty, Deputy Director of the ETH Zurich Think Tank, explains why resilience is less about avoiding individual crises and more about preparedness, sound judgment and understanding interdependencies

Prof. Dr. Reto Eberle (RE): *The Center for Security Studies (CSS) at ETH Zurich examines security policy and sociotechnical risks. What exactly does the CSS do and what is your role there?*

Dr. Myriam Dunn Cavelty (MDC): The CSS is more than a Think Tank. We are a center of competence for international and Swiss security policy. Since 2022 we have held a national mandate on behalf of the Swiss Confederation built on four pillars: teaching and continuing education, research, support for junior researchers, and policy consultancy. My own work spans all four areas. In my research, I focus primarily on digital technologies at the intersection with security policy, including cybersecurity,

international politics and the question of how technologies change politics and society. My teaching includes cybersecurity policy and I am also a lecturer in the political science master's program. In addition, I am involved in continuing education and provide coaching and mentoring to junior researchers. I have worked with the Federal Administration as a policy consultant for many years, currently on issues such as cybersecurity, digital sovereignty and integrating scientific expertise into crisis management. This interplay is precisely what makes the CSS special; our combination of research, teaching, support for the next generation of researchers and consultancy is beneficial beyond the boundaries of these individual areas.





Matthias Bossardt (MB): *How do scientific findings make their way to decision-makers in politics and business in practice?*

MDC: Our consultancy model is based on dialog. We do not just publish reports. We work with federal agencies and, in some cases, cantonal authorities, create platforms for exchange, run workshops and bring stakeholders together across institutional silos. Anticipation is particularly important: we strive to build expertise before an issue becomes urgent. At the same time, we step back as soon as a process reaches the stage of debate between political parties. For us, measuring impact is less about download figures than about qualitative indicators. Do our analyses inform decision-making? Are they featured in parliamentary initiatives or referenced internationally? What matters most is the trust built over many years while maintaining our academic freedom.

RE: *Which risks pose the greatest challenges to Switzerland's resilience today?*

MDC: Individual risks such as pandemics, power shortages or armed conflicts are generally analyzed quite well. The greater challenge, however, lies in what happens when they coincide. In international politics, we talk about "polycrises" or "polyrisks" – risks that occur simultaneously, reinforce one another or trigger cascading effects. Switzerland's high degree of interconnectedness is both a strength and a vulnerability. Digital systems, supply chains, energy supplies, financial systems and societal responses are closely interlinked. Yet these interactions are difficult to capture in conventional analyses of individual risks.

RE: *That sounds a bit like the financial crisis. Many individual risks were known, but their interconnectedness was underestimated. What are the implications for preparedness?*

MDC: It is important to run exercises based on complex scenarios. With sociotechnical risks in particular, the outcome depends not only on the event itself but also on how society, organizations and policymakers respond. Exercises help reveal these dynamics. However, they also take time and resources, and sometimes yield uncomfortable findings. That is why practice alone is not enough; the lessons learned must also be put into action consistently. This is a pain point for institutions, because preventive investments are an upfront cost, while their benefits only become apparent when a crisis strikes.





“Cyber threats have gone from exceptional events to constant background noise.”

MB: *What role does “critical infrastructure” play in this context and how is it defined?*

MDC: Critical infrastructure refers to systems, services or facilities whose failure would have serious consequences for the population, the state, society or the economy. But the key question is not just what is important, but what actually becomes critical. What impact would a failure have? What dependencies and cascading effects would arise? Are alternatives available? Much of this infrastructure is privately owned, so cooperation between the public and the private sectors is essential. Infrastructure that supports multiple sectors, such as electricity and digital networks, is particularly relevant because so many other functions depend on it. The difficulty is that companies are not always sufficiently aware of their own role in, or dependencies on, the wider system.

RE: *Electricity is one example of infrastructure that supports multiple sectors. How well is Switzerland protected against blackouts or power shortages?*

MDC: It is difficult to give a clear answer, because even “adequately protected” is hard to define and resilience often only becomes apparent when an event occurs. It is important to distinguish between a blackout, a local power outage and a power shortage. Since 2022, preparedness for shortages has been strengthened through measures such as reserves, emergency planning and greater public awareness. At the same time, some companies are running very practical exercises to explore what would happen during a prolonged outage. Which sites would remain open? How would goods be distributed? What would happen if payment systems failed? How would they coordinate with the authorities? Such exercises show what resilience looks like in practice. Preparedness is therefore by no means solely a government responsibility.

MB: *Cyberattacks now affect businesses and nation-states alike. What are the greatest challenges for Switzerland?*

MDC: Cyber threats have gone from exceptional events to constant background noise. Criminal ransomware attacks, for example, continue to cause significant damage. Small and medium-sized enterprises in particular struggle to keep pace with increasingly professional attackers. In hybrid conflicts, cyberspace is particularly well suited to causing disruption and sowing doubt. Attribution is possible, but it takes time and resources. This makes cyberspace an effective arena for creating uncertainty and undermining trust.

MB: *How resilient is Switzerland's critical infrastructure to these threats?*

MDC: It varies considerably. Some large organizations with substantial resources have excellent capabilities, while smaller companies have far fewer. Switzerland has skilled professionals, strong educational institutions and businesses, and substantial financial resources. Even so, I would not say that we are sufficiently resilient overall. It is not just about individual cyberattacks. Technical risks can be managed to some extent through sound risk management and business continuity planning. Dependencies and the psychological dimension are more difficult to address. People need to be able to trust that systems generally work. When that trust erodes, society also becomes more vulnerable.

RE: *Does this uncertainty come mainly from deliberate attempts to influence people, or is it something that arises within society itself?*

MDC: Both. Some actors exploit or amplify uncertainty. At the same time, we are seeing a broader loss of trust and a more pessimistic outlook on the future. Vague fears are particularly difficult to address. A specific concern can be met with information. But when people no longer know whom or what to believe, it is not enough to simply say "That's not true." We now observe this even with images. In the past, people generally assumed they were genuine; today, the first reaction is often to suspect manipulation. This erosion of our ability to verify information and trust what we see and hear is a major challenge.

RE: *What does digital sovereignty mean for Switzerland in practice?*

MDC: Digital sovereignty does not mean complete independence; there is no such thing. Dependencies are not inherently bad either, because they enable efficiency, cooperation and specialization. What matters is that they are recognized and assessed. An organization needs to know which tasks are critical and which resources they depend on: software, hardware, data, cloud services, know-how or operational expertise. The next question is what happens if a provider experiences an outage, raises prices dramatically or becomes insolvent. The organization also needs to assess additional risks arising, for example, from geopolitical developments. Technical mapping alone is therefore not enough.

"Crisis exercises alone are not enough; the lessons learned must also be put into action consistently."

MB: *What else is needed?*

MDC: Sound risk management. Which risks are we able and willing to bear? Where does redundancy make sense, and where would an alternative be disproportionately expensive? These questions need to be addressed by interdisciplinary teams, rather than by IT alone. We still have too few professionals capable of bringing multiple perspectives together. A lot of learning only happens in practice. Education and training are not yet systematically aligned with these interdisciplinary questions either.

MB: *Which societal values are coming under pressure from digital technologies, particularly AI?*

MDC: Trust is under considerable pressure, as are privacy, data sovereignty and autonomy. There are also questions of equal treatment and availability. People with access to better AI tools can gain advantages in education and secure a competitive edge. At the same time, values such as explainability, responsibility and the ability to challenge decisions are becoming more important. When an AI system makes a recommendation, a person must be able to understand, or at least follow, the reasoning behind it. Automation bias is particularly concerning. Automated outputs are convenient, and this convenience creates a risk that humans remain the decision-makers in name but, in practice, merely approve what the machine has prepared. Organizations therefore need deliberate checkpoints where people can scrutinize and challenge outputs.

RE: *We see this in education too. AI can do an excellent job of preparing material, but it can be tempting to treat that material as the finished result. What can we do to ensure we still develop sound judgment?*

MDC: This requires fundamental knowledge and a conscious effort to practice critical thinking. Without a grasp of the basics, people can no longer assess a system's output. Schools, universities and companies therefore need to adapt how they teach and assess learning. AI is here to stay. The question is how to empower people to use AI effectively while critically evaluating what it produces. This is also a matter of equal opportunity. Access, support and skills must not become a new social dividing line.





MB: *Critical thinking takes time and energy. To what extent does a slower pace play a role in this, as we see, for example, in some political decision-making processes in Switzerland?*

MDC: For democracies, a slower pace can be a positive quality. Deliberating, listening to different perspectives and consciously introducing friction all take time. This is why it is so important not to accelerate certain decisions in a world where everything is speeding up. This mindset can also be built into the technology itself. Systems can be designed so that not every decision can be made immediately. Sometimes friction is a safety feature.

RE: *That is why, in auditor training, we deliberately experiment with analog formats such as paper-based work, scenarios or discussion. Our aim is not to counter the technology, but to develop independent thinking.*

MDC: Exactly. Critical thinking is becoming more important, not less, in the AI era.

RE: *Where is action on AI most urgently needed: regulation, institutional resilience or public awareness?*

MDC: In all three areas equally. Regulation and self-regulation are important, but they will not be enough. What matters most is how AI is integrated into institutions. How does it change workflows and professional roles? Who is accountable? What happens if systems suddenly go down? The more deeply AI is embedded in industrial processes, energy supplies or other critical areas, the more important it is that we can cope with outages and have alternatives available. At the same time, we need

a broad public discussion about the world of work, education, responsibility and governance. I am not pessimistic about this. People and institutions have adapted to technological upheavals before. We can use AI productively, but access and skills must not create further inequalities.

MB: *Disinformation and foreign interference repeatedly pop up as topics of debate around elections and referendums. What do we know about their impact?*

MDC: Disinformation attempts and campaigns that can be attributed to specific actors do exist, even in Switzerland. They do not come solely from foreign sources, though; domestic actors can also distort information. The question about impact is much harder to answer. From a research perspective, it is difficult to get reliable data on how much a particular campaign changes behavior. People often seek information that aligns with their existing views, so beliefs tend to be reinforced rather than completely reversed. But sowing doubt can itself have a significant impact. It erodes trust to be constantly told that you are being manipulated and cannot rely on anything anymore. That is why we should avoid sensationalizing every attempt at disruption and focus instead on strengthening media literacy and societal resilience. It comes down to the ability to put information in context, check sources and tolerate uncertainty.





RE: *Bringing these themes together, where is action most urgently needed in Switzerland?*

MDC: First, we need to explain more clearly what resilience actually means. It is not just a quality of individual organizations or people, but a task for society as a whole. It is about preparedness. People need to know what to do in a crisis; this revolves around information, emergency planning and practical exercises. Second, we need to break down silos. Energy, cybersecurity, supplies and public administration cannot be considered in isolation. Preparedness must take a cross-sector approach involving the federal government, cantons, municipalities and the private sector. Third, we need to do more to anticipate risks. I do not mean precise predictions, but continuous horizon scanning and monitoring of dependencies and risk combinations. If we want to be resilient, we need to take a systemic view of ourselves. The real problem is often not a lack of knowledge, but a lack of action.

MB: *Who exactly is the “we” you refer to when you say “we need to?”*

MDC: Society as a whole. And this is the very challenge. It is easy to shift responsibility onto others. People are reluctant to change their behavior as long as the need to act remains abstract.

RE: *Perhaps that is why a decentralized structure that involves the local level is particularly important. When risks become concrete and we understand where resistance arises, an abstract issue becomes something tangible.*

MDC: Yes. Local initiatives, events, exercises and concrete scenarios can be very effective. Incentives often work better than compulsion. The key task is to raise awareness so that people understand for themselves why preparedness makes sense. One of our studies on emergency preparedness showed that a substantial proportion of the population is unsure even about basic questions, such as what to do when a warning siren sounds. Resilience therefore does not start with a crisis management team. It begins well before that, in everyday life.

RE: *Thank you very much for the interview.*

Prof. Dr. Reto Eberle

Partner, Member of Department of Professional Practice
KPMG Switzerland

Dr. Matthias Bossardt

Partner, Head Risk Consulting Services
KPMG Switzerland

This article is part of KPMG’s Board Leadership News, our newsletter for board members. It is published three times a year.

About the KPMG Board Leadership Center

The KPMG Board Leadership Center offers support and guidance to board members. We equip you with the tools and insights you need to be highly effective in your role, enabling you to focus on the issues that really matter to you and your business. In addition, we help you to connect with peers and exchange experiences.

Learn more at kpmg.ch/blc

Subscribe to the Board Leadership Newsletter: [Register here](#)

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received, or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation. The scope of any potential collaboration with audit clients is defined by regulatory requirements governing auditor independence. If you would like to know more about how KPMG AG processes personal data, please read our [Privacy Policy](#), which you can find on our homepage at www.kpmg.ch.

© 2026 KPMG AG, a Swiss corporation, is a group company of KPMG Holding LLP, which is a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.